Article:
Ghalaii, M, Ottaviani, C, Kumar, R et al. (2 more authors) (2020) Long-Distance Continuous-Variable Quantum Key Distribution With Quantum Scissors. IEEE Journal of Selected Topics in Quantum Electronics, 26 (3). 6400212. ISSN 1077-260X

https://doi.org/10.1109/jstqe.2020.2964395

Long-distance continuous-variable quantum key distribution with quantum scissors

Masoud Ghalaii,[1] Carlo Ottaviani,[2] Rupesh Kumar,[3] Stefano Pirandola,[2,4] and Mohsen Razavi[1]

[1]*Faculty of Engineering and Physical Sciences, University of Leeds, Leeds LS2 9JT, United Kingdom*
[2]*Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, United Kingdom*
[3]*Department of Physics, University of York, York YO10 5DD, United Kingdom*
[4]*Research Laboratory of Electronics, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA*

We investigate the use of quantum scissors, as candidates for non-deterministic amplifiers, in continuous-variable quantum key distribution. Such devices rely on single-photon sources for their operation and as such, they do not necessarily preserve the Guassianity of the channel. Using exact analytical modeling for the system components, we bound the secret key generation rate for a protocol that uses quantum scissors. We find that, for certain non-zero values of excess noise, such a protocol can reach longer distances than the counterpart with no amplification. This sheds light into the prospect of using quantum scissors as an ingredient in continuous-variable quantum repeaters.

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] addresses the problem of sharing secret keys between two users. Such keys can then be used for secure communications. While original QKD protocols [2–5] rely on encoding classical bits of information in discrete quantum states, such as the polarization of single photons, one can also exploit continuous-variable QKD (CV QKD) protocols, where the bits are encoded on the quadratures of light [6–9]. In particular, the recent progress in CV QKD systems has placed them in a competitive position with their conventional discrete-variable counterparts [10, 11]. For instance, contrary to discrete-variable QKD protocols, which require single-photon detectors, CV QKD uses coherent measurement schemes, such as homodyne and/or heterodyne detection, to measure light quadratures, compatible with high-rate coherent telecommunications systems [12–14]. Moreover, CV QKD protocols can be the better choice over short distances than the metropolitan zones [11]. Once it comes to long distances, however, CV QKD has its own challenges to compete with discrete-variable QKD [15]. This paper examines how the security distance can be enhanced in CV QKD systems by using realistic non-deterministic amplification [16].

One of the proposed solutions to improve the rate-versus-distance performance of CV QKD protocols is to use noiseless linear amplifiers (NLAs) [16, 17]. It is known that deterministic amplification cannot be noise free [18]. An NLA can only then work *probabilistically*. This inevitably reduces the key rate by a factor corresponding to the success rate of the NLA, which implies that, at short distances, the use of NLAs may not be beneficial. The key rate may, however, increase at long distances because of the improvement in the signal to noise ratio. That is, while the number of data points we can use for key extraction is less, the quality of the remaining points could be also high, such that a larger number of secret key bits can be extracted. This has been shown theoretically by treating the NLA as a probabilistic, but noiseless, black box, where an upper bound on success probability, $1/g^2$ with g being the amplification gain, was used [16].

The story can be quite different when we replace the above ideal NLA with realistic systems that offer NLA-like functionality. For instance, one of the most basic structures for an NLA is a quantum scissor (QS), which combines the incoming light with a single photon [19, 20]. While under weak signal assumptions, a QS can be approximated as an NLA, more precise analysis reveals that its operation is not necessarily noiseless. This is particularly important because in many CV QKD protocols the transmitted signal does not have a fixed intensity, and realistic NLAs often treat different input signals differently. This is more or less true for other proposals that implement the NLA operation [21–26].

In this paper, we provide a realistic account of what a QS can offer within a CV QKD setup. In particular, using an exact model for the QS setup, we analyze the secret key rate of a Gaussian modulated protocol, whose receiver unit is equipped with a QS. One of the implications of our exact modeling for the QS is that we cannot directly apply standard key rate calculation techniques that rely on the Gaussianity of the output states. This will make the exact calculation of the key rate cumbersome. We manage this problem by using relevant bounds for certain components of the key rate. We investigate the extent at which the use of quantum scissors can increase the security distance in CV QKD systems.

One of our key incentives for carrying out the above analysis is to provide insights into the applicability of other proposals for CV quantum repeaters [27–29] for QKD operation. The QS-equipped CV QKD link that we consider here contains the elementary repeater (error correction) link used in the repeater setup of [27], and as such a poor performance for this basic building block could cast shadow on the usefulness of any larger quantum repeater setup that relies on such elementary links. In the repeater setup of [27], CV teleportation is used to swap entanglement between already entangled links, represented by QM1-QM2 and QM3-QM4 in Fig. 1. Each of such links have been entangled by sending one half of a two-mode squeezed vacuum state, represented by EPR boxes, through a lossy channel. The received signal will then be amplified, in a probabilistic way, by the QS module, and will be stored in the corresponding quantum memory (QM). Note that, considering the non-deterministic behavior of the QS, use of QM modules is necessary if we want to achieve any rate enhancement from our repeater setup. The dual homodyne module will then effectively perform entanglement

FIG. 1. A two-leg quantum repeater module as proposed in [27]. Each leg is composed of an EPR source generating two-mode squeezed vacuum states, a quantum scissor (QS), and two quantum memory (QM) units. Beam splitters with transmissivity T characterize the loss in each leg, with excess noise represented by ε. Upon successful operation of the QS in each leg, the output of the QS and the EPR source are stored in respective quantum memories. When both legs are ready, a joint dual homodyne (Dual Hom) measurement is performed on the quantum states stored in QM2 and QM3, which swaps entanglement to QM1 and QM4.

swapping in the CV domain once both links have had successful QS operations.

Note that the above repeater setup must use a *physical* QS implementation, and not a virtual one, in order to offer any rate advantage. That is, the class of measurement-based NLA (MB-NLA) implementations [30–32], which rely on data post-selection, would not be suitable for such CV repeaters. Due to reliance of MB-NLAs on classical post-selection, the state of QM2 and QM4 must effectively be measured before the entanglement swapping can be done. Even if we do not consider the applications of our considered setup in CV repeater settings, one must be cautious with typically poor success probability of MB-NLAs compared to that of physical NLAs [33]. This suggests that the use of physical NLAs in CV QKD systems is still of interest, and, in fact, one may favour a physical realization of an NLA over its virtual post-measurement implementation due to restrictions on the MB-NLA [34]. Our work here would shed more light into the applicability of such physical realizations by offering an accurate analysis of the underlying system.

The manuscript is structured as follows. In Sec. II, we describe details of the proposed system. In Sec. III, by analyzing input-output characteristic functions of a single QS, we calculate the exact output state and success probability of the QS NLA in [20]. We also study the non-Gaussian behavior of this system. In Sec. IV, we present the key rate analysis of the CV QKD link with a single QS as part of its receiver. In Sec. V, we discuss the numerical results. Finally, Sec. VI concludes the paper.

II. SYSTEM DESCRIPTION

In this section, we describe our proposed setup for the QS-amplified CV QKD protocol. We assume that the sender, Alice (A), is connected to the receiver, Bob (B), via a quantum channel; see Fig. 2(a). The protocol runs along the same lines as proposed by Grosshans and Grangier in 2002 (GG02) [6, 7, 35, 36]. That is, in every round, Alice transmits a coherent state $|\alpha\rangle$ to Bob, where $\alpha = x_A + ip_A$, with real parameters x_A and p_A being chosen randomly according to the

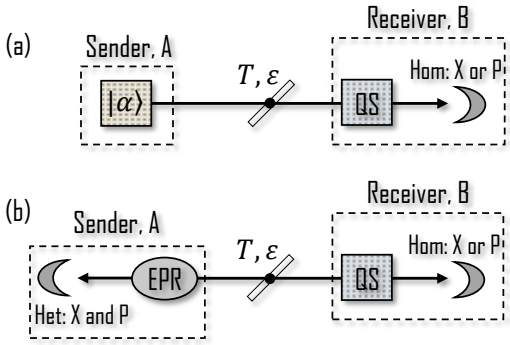

FIG. 2. (a) Schematic view of CV QKD link with an additional quantum scissor at the receiver. (b) Entanglement-based CV QKD protocol equivalent to (a). Hom and Het represent, respectively, the homodyne detection and heterodyne detection modules.

following Gaussian probability density functions:

$$f_{X_A}(x_A) = \frac{e^{-\frac{x_A^2}{V_A/2}}}{\sqrt{\pi V_A/2}} \quad \text{and} \quad f_{P_A}(p_A) = \frac{e^{-\frac{p_A^2}{V_A/2}}}{\sqrt{\pi V_A/2}}, \quad (1)$$

where V_A is the modulation variance in the shot-noise units. At the receiver, however, we equip Bob with a single QS before the homodyne module used in GG02. Upon a successful QS operation, Bob randomly chooses to measure $\hat{x}_B = \hat{a}_B + \hat{a}_B^\dagger$ or $\hat{p}_B = (\hat{a}_B - \hat{a}_B^\dagger)/i$, where $\hat{a}_B$ represents the annihilation operator for the output mode of the QS. During the sifting stage, Bob would then publicly declare his measurement choices as well as the rounds in which the QS has been successful. Alternatively, one can use the equivalent entanglement-based (EB) scheme of Fig. 2(b), where Alice's source is replaced with an EPR source followed by heterodyne detection on one of the two modes of the state (by EPR source we mean a two-mode squeezed vacuum state [9]). In either case, we assume that Bob can reconstruct, in an error-free way, the phase reference for the local oscillator used in his homodyne detection. By using post-processing techniques, Alice and Bob extract a key from the subset of data for which the QS has been successful.

Quantum scissors are the main building blocks in the NLA proposed by Ralph and Lund [20]. At the core of a QS, there is a partial Bell-state measurement (BSM) module, with a balanced beam splitter followed by two single-photon detectors, in the space spanned by number states $|0\rangle$ and $|1\rangle$. This BSM module is driven by an asymmetric entangled state $|\psi\rangle = \sqrt{\mu}|1\rangle_{\hat{c}}|0\rangle_{\hat{b}_3} + \sqrt{1-\mu}|0\rangle_{\hat{c}}|1\rangle_{\hat{b}_3}$, generated by a single photon that goes through a beam splitter with transmittance μ; see Fig. 3. For an input state in the $|0\rangle$-$|1\rangle$ space, the QS could then offer an asymmetric teleportation functionality, whenever the BSM operation is successful, i.e., when only one of D1 or D2 detector in Fig. 3 clicks. For instance, in the particular case of a weak coherent state input $|\alpha\rangle_{\hat{a}_1} \approx |0\rangle_{\hat{a}_1} + \alpha|1\rangle_{\hat{a}_1}$, with $|\alpha| \ll 1$, a single click could come from the single-photon component in the entangled state $|\psi\rangle$ and/or the input state. In that case, the output state, after renormalization, can be approximated by $|0\rangle_{\hat{b}_3} + \alpha g|1\rangle_{\hat{b}_3} \approx |\alpha g\rangle_{\hat{b}_3}$, for $|g\alpha| \ll 1$, where

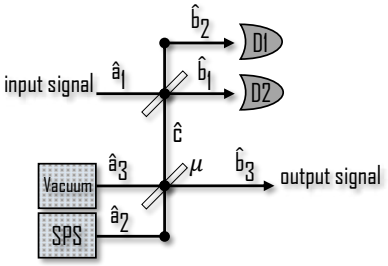

FIG. 3. The schematic diagram of a quantum scissor. Here, we assume that an on-demand ideal single-photon source (SPS) is in use, and that the single-photon detectors have unity efficiencies.

$g = \sqrt{(1-\mu)/\mu}$ represents the amplification gain of the QS. Under these assumptions, the success probability for the QS operation is given by $P_{\rm succ}^{\rm RL}(\alpha) \approx \mu + (1-\mu)|\alpha|^2$. Note that, in the above description, the essential assumption for a QS to possibly operate as an NLA is that $|\alpha| \ll 1$.

There are two reservations in using the above asymptotic approach for analyzing a QS-based CV QKD system. First, note that the output state of a QS is always in the space spanned by single-photon and vacuum states. By approximating the output state as a coherent state, we are introducing some errors, which can affect the security of the system. More precisely, the transition from a coherent state to a single-photon state is a non-Gaussian one, whose effect must be carefully considered in the security analysis. Secondly, in the GG02 protocol, the coherent states are chosen randomly via Gaussian distributions; hence, the input states to the QS may not necessarily satisfy the assumption $|\alpha| \ll 1$.

In order to resolve the above issues, in our work, we find the *exact* output state and probability of success for an arbitrary coherent state at the input of a QS. This will be detailed in Sec. III. We note that one can implement a QS/NLA which truncates input states to first N Fock states [37, 38]. Here we limit ourselves to the single-photon truncation. We then apply our findings to the key rate analysis of a QS-equipped CV QKD system. For simplicity, we assume that the required single-photon source (SPS) in the QS is ideal and on-demand. Single-photon detector efficiencies are also assumed to be unity. Our analysis can, nevertheless, be extended to account for the imperfections in the source and detectors.

III. QUANTUM SCISSORS: INPUT-OUTPUT RELATIONSHIP

In this section, we first obtain an exact input-output relationship for a QS driven by a coherent state. We use characteristic functions to model the input and output states. For a joint, M-mode, state $\hat{\rho}$, where each mode j is represented by an annihilation operator $\hat{a}_j$, the antinormally-ordered characteristic function is given by

$$\chi_{\rm A}^{\hat{\rho}}(\xi_1,\ldots,\xi_M) = \Big\langle \bigotimes_{j=1}^{M} \hat{D}_{\rm A}(\hat{a}_j,\xi_j) \Big\rangle_{\hat{\rho}}, \tag{2}$$

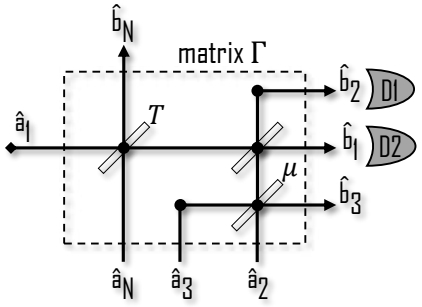

FIG. 4. The quantum channel and the QS are considered as a combined system with input modes $\hat{a}_1 - \hat{a}_3$ and $\hat{a}_{\rm N}$ and output modes $\hat{b}_1 - \hat{b}_3$ and $\hat{b}_{\rm N}$. The transformation matrix of the system is given by (4).

where $\langle\circ\rangle_{\hat{\rho}} \equiv {\rm tr}[\hat{\rho}\circ]$ and $\hat{D}_{\rm A}(\hat{a},\xi) = e^{-\xi^*\hat{a}}e^{\xi\hat{a}^\dagger}$ is the antinormally-ordered displacement operator with ξ^* being the complex conjugate of the complex number $\xi = \xi_r + i\xi_i$, with ξ_r and ξ_i are real numbers. The density matrix $\hat{\rho}$ and its antinormally-ordered characteristic function are connected via a Fourier-transform as follows

$$\hat{\rho} = \int \frac{d^2\xi_1}{\pi} \cdots \int \frac{d^2\xi_M}{\pi} \chi_{\rm A}^{\hat{\rho}}(\xi_1,\ldots,\xi_M) \bigotimes_{j=1}^{M} \hat{D}_{\rm N}(\hat{b}_j,\xi_j), \tag{3}$$

where $\hat{D}_{\rm N}(\hat{a},\xi) = e^{\xi\hat{a}^\dagger}e^{-\xi^*\hat{a}}$ is the normally-ordered displacement operator and $\int d^2\xi = \int_{-\infty}^{+\infty} d\xi_r \int_{-\infty}^{+\infty} d\xi_i$.

In the following, we use the above formulation to analyze the setup in Fig. 4, which includes a QS driven by an arbitrary coherent state through a lossy channel with transmissivity T and excess noise ε.

A. Pre-measurement state

For the setup in Fig. 4, we can use the well-known relationships for beam splitters to relate the four input modes to the four output modes. The dashed box Γ is a linear optics circuit, for which such input-output relationships can be obtained. In particular, considering the input modes represented by $\mathcal{A}^T = [\hat{a}_1\ \hat{a}_2\ \hat{a}_3\ \hat{a}_{\rm N}]$ and output modes $\mathcal{B}^T = [\hat{b}_1\ \hat{b}_2\ \hat{b}_3\ \hat{b}_{\rm N}]$, we find $\mathcal{B} = \Gamma\mathcal{A}$, where the transformation matrix

$$\Gamma = \begin{pmatrix} \sqrt{\frac{T}{2}} & \sqrt{\frac{\mu}{2}} & -\sqrt{\frac{1-\mu}{2}} & \sqrt{\frac{1-T}{2}} \\ -\sqrt{\frac{T}{2}} & \sqrt{\frac{\mu}{2}} & -\sqrt{\frac{1-\mu}{2}} & -\sqrt{\frac{1-T}{2}} \\ 0 & \sqrt{1-\mu} & \sqrt{\mu} & 0 \\ -\sqrt{1-T} & 0 & 0 & \sqrt{T} \end{pmatrix} \tag{4}$$

is a unitary orthogonal matrix, i.e., $\Gamma^{\rm T} = \Gamma^{-1}$. The output antinormally-ordered characteristic function can then be ex-

pressed in terms of the input one by

$$\begin{aligned}\chi_{\rm A}^{\rm out}(\xi_1,\xi_2,\xi_3,\xi_{\rm N}) =&\Big\langle \prod_{m=1}^{3}\hat{D}_{\rm A}(\hat{b}_m,\xi_m)\hat{D}_{\rm A}(\hat{b}_{\rm N},\xi_{\rm N})\Big\rangle\\ =&\Big\langle \prod_{m=1}^{3}\hat{D}_{\rm A}(\hat{a}_m,\lambda_m)\hat{D}_{\rm A}(\hat{a}_{\rm N},\lambda_{\rm N})\Big\rangle\\ =&\chi_{\rm A}^{\rm in}(\lambda_1,\lambda_2,\lambda_3,\lambda_{\rm N}),\end{aligned} \tag{5}$$

where $[\lambda_1\ \lambda_2\ \lambda_3\ \lambda_{\rm N}]^{\rm T} = \Gamma^{\rm T}[\xi_1\ \xi_2\ \xi_3\ \xi_{\rm N}]^{\rm T}$, with $\Gamma^{\rm T}$ being the transpose of Γ. Here, we make use of the fact that $\hat{D}_{\rm A}(s\hat{a},\xi) = \hat{D}_{\rm A}(\hat{a},s\xi)$, $s\in\mathbb{R}$, and $\langle\hat{D}_{\rm A}(\hat{a},\xi_1)\hat{D}_{\rm A}(\hat{a},\xi_2)\rangle = e^{\xi_1\xi_2^*}\langle\hat{D}_{\rm A}(\hat{a},\xi_1+\xi_2)\rangle$.

Next, we consider the particular input state

$$\hat{\rho}_{\rm in} = |\alpha\rangle_{\hat{a}_1}\langle\alpha|\otimes|1\rangle_{\hat{a}_2}\langle 1|\otimes|0\rangle_{\hat{a}_3}\langle 0|\otimes\int d^2\beta f_\varepsilon(\beta)|\beta\rangle_{\hat{a}_{\rm N}}\langle\beta|, \tag{6}$$

where $f_\varepsilon(\beta) = \frac{e^{-\frac{|\beta|^2}{\varepsilon/2}}}{\pi\varepsilon/2}$, with ε being the channel excess noise. This corresponds to a Gaussian attack by Eve, enabled by an entangling cloner [39], which we later use in forthcoming sections. For the above set of input states, the output characteristic function has the following expression

$$\begin{aligned}\chi_{\rm A}^{\rm out}(\xi_1,\xi_2,\xi_3,\xi_{\rm N}) =&{\rm tr}\big[\hat{\rho}_{\rm in}\hat{D}_{\rm A}(\hat{a}_1,\lambda_1)\hat{D}_{\rm A}(\hat{a}_2,\lambda_2)\\ &\hat{D}_{\rm A}(\hat{a}_3,\lambda_3)\hat{D}_{\rm A}(\hat{a}_{\rm N},\lambda_{\rm N})\big].\end{aligned} \tag{7}$$

By using the transformation matrix Γ, this can be re-written as the following

$$\begin{aligned}\chi_{\rm A}^{\rm out}(\xi_1,\xi_2,\xi_3,\xi_{\rm N}) =&e^{-\frac{T}{2}|\xi_1-\xi_2-\sqrt{2}\tau\xi_{\rm N}|^2}\\ &\times e^{\sqrt{2T}i{\rm Im}[\bar{\alpha}(\xi_1-\xi_2-\sqrt{2}\tau\xi_{\rm N})]}\\ &\times e^{-\frac{1-T}{2}(1+\frac{\varepsilon}{2})|\xi_1-\xi_2+\frac{\sqrt{2}}{\tau}\xi_{\rm N}|^2}\\ &\times e^{-\frac{1-\mu}{2}|\xi_1+\xi_2-\frac{\sqrt{2}}{g}\xi_3|^2}\\ &\times e^{-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2}\\ &\times\Big(1-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2\Big),\end{aligned} \tag{8}$$

where $g=\sqrt{(1-\mu)/\mu}$, $\tau=\sqrt{(1-T)/T}$, and ${\rm Im}[\xi]$ being the imaginary part of complex number ξ. Using (3), the joint state of the output modes is then given by

$$\begin{aligned}\hat{\rho}_{\mathcal{B}} =&\int\frac{d^2\xi_1}{\pi}\int\frac{d^2\xi_2}{\pi}\int\frac{d^2\xi_3}{\pi}\int\frac{d^2\xi_{\rm N}}{\pi}\chi_{\rm A}^{\rm out}(\xi_1,\xi_2,\xi_3,\xi_{\rm N})\\ &\hat{D}_{\rm N}(\hat{b}_1,\xi_1)\hat{D}_{\rm N}(\hat{b}_2,\xi_2)\hat{D}_{\rm N}(\hat{b}_3,\xi_3)\hat{D}_{\rm N}(\hat{b}_{\rm N},\xi_{\rm N}).\end{aligned} \tag{9}$$

We can next trace out mode $\hat{b}_{\rm N}$ to obtain the joint state of $[\hat{b}_1\ \hat{b}_2\ \hat{b}_3]$, which is

$$\begin{aligned}\hat{\rho}_{\rm out} =&\int\frac{d^2\xi_1}{\pi}\int\frac{d^2\xi_2}{\pi}\int\frac{d^2\xi_3}{\pi}\chi_{\rm A}^{\rm out}(\xi_1,\xi_2,\xi_3,0)\\ &\hat{D}_{\rm N}(\hat{b}_1,\xi_1)\hat{D}_{\rm N}(\hat{b}_2,\xi_2)\hat{D}_{\rm N}(\hat{b}_3,\xi_3),\end{aligned} \tag{10}$$

where

$$\begin{aligned}\chi_{\rm A}^{\rm out}(\xi_1,\xi_2,\xi_3,0) =&e^{-F_1|\xi_1-\xi_2|^2}e^{\sqrt{2T}i{\rm Im}[\bar{\alpha}(\xi_1-\xi_2)]}\\ &\times e^{-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2}e^{-\frac{1-\mu}{2}|\xi_1+\xi_2-\frac{\sqrt{2}}{g}\xi_3|^2}\\ &\times\big(1-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2\big),\end{aligned} \tag{11}$$

with $F_1 = \frac{1}{2}+\frac{1}{4}(1-T)\varepsilon$. Note that $\varepsilon_{\rm rec} = (1-T)\varepsilon$ is the amount of excess noise at the receiver side; thus, $F_1 = \frac{1}{2}+\frac{1}{4}T\varepsilon_{\rm tm}$, where $\varepsilon_{\rm tm} = \varepsilon_{\rm rec}/T$ is the amount of excess noise at the transmitter.

B. Post-selected state

Following [20], we consider a QS to be successful if only one detector in Fig. 4 clicks. In order to model such measurements we use the following non-resolving measurement operator

$$\hat{M} = (\mathbb{1}-|0\rangle_1\langle 0|)\otimes|0\rangle_2\langle 0|, \tag{12}$$

which corresponds to the case where detector D1 clicks while D2 does not. The post-selected state, $\hat{\rho}_{\rm out}^{\rm PS}$, is then given by [40]:

$$\begin{aligned}\hat{\rho}_{\rm out}^{\rm PS} =&\frac{{\rm tr}_{\hat{b}_1\hat{b}_2}(\hat{\rho}_{\rm out}\hat{M})}{{\rm tr}(\hat{\rho}_{\rm out}\hat{M})}\\ =&\frac{1}{P^{\rm PS}}\int\frac{d^2\xi_1}{\pi}\int\frac{d^2\xi_2}{\pi}\int\frac{d^2\xi_3}{\pi}\chi_{\rm A}^{\rm out}(\xi_1,\xi_2,\xi_3,0)\\ &\times(\pi\delta^2(\xi_1)-1)\hat{D}_{\rm N}(\hat{b}_3,\xi_3),\end{aligned} \tag{13}$$

where $\delta^2(\xi)=\delta(\xi_r)\delta(\xi_i)$ and $P^{\rm PS}={\rm tr}(\hat{M}\hat{\rho}_{\rm out})$ is the corresponding (success) probability of the measurement $\hat{M}$, which will be calculated in Sec. III C.

Because the truncated post-measurement state lives in the qubit subspace spanned by number states $\{|0\rangle_{\hat{b}_3},|1\rangle_{\hat{b}_3}\}$, the output state has the form

$$\begin{aligned}\hat{\rho}_{\rm out}^{\rm PS}(\alpha) =&\rho_{00}(\alpha)|0\rangle_{\hat{b}_3}\langle 0|+\rho_{01}(\alpha)|0\rangle_{\hat{b}_3}\langle 1|\\ &+\rho_{10}(\alpha)|1\rangle_{\hat{b}_3}\langle 0|+\rho_{11}(\alpha)|1\rangle_{\hat{b}_3}\langle 1|,\end{aligned} \tag{14}$$

where $\rho_{jk}(\alpha) = {}_{\hat{b}_3}\langle j|\hat{\rho}_{\rm out}^{\rm PS}(\alpha)|k\rangle_{\hat{b}_3}$, for $j,k=0,1$. We then obtain

$$\begin{cases}\rho_{00}(\alpha) = \frac{2[2F_1(2F_1+1)+T|\alpha|^2]}{(g^2+1)(2F_1+1)^3}e^{-T\frac{|\alpha|^2}{2F_1+1}}/P^{\rm PS}(\alpha)\\ \rho_{01}(\alpha) = \frac{-2g\sqrt{T}\alpha}{(g^2+1)(2F_1+1)^2}e^{-T\frac{|\alpha|^2}{2F_1+1}}/P^{\rm PS}(\alpha) = \rho_{10}^*(\alpha)\\ \rho_{11}(\alpha) = \frac{2g^2}{g^2+1}\Big(\frac{e^{-T\frac{|\alpha|^2}{2F_1+1}}}{2F_1+1}-\frac{e^{-T\frac{|\alpha|^2}{2F_1}}}{4F_1}\Big)/P^{\rm PS}(\alpha).\end{cases} \tag{15}$$

We remark that in the case that only detector D2 clicks, the QS is still considered successful. After working out the post-selected output state, we find that the result has the same form as in (14), but we only need to replace α with $-\alpha$ in (15). In practice, in a QKD setup, Bob can negate its measurement

results whenever this happens. One can also use a unitary operation to correct the output state so that we always end up with (14) as the post-selected state.

We note that the post-measurement state is Hermitian and positive-semidefinite, as expected. In addition, in the limit of $|g\alpha| \ll 1$, we can verify that the post-selected state of the single QS approaches the weak coherent state $|g\alpha\rangle$.

C. Probability of success

The probability of success for measurement $\hat{M}$ and input $|\alpha\rangle$ is given by

$$\begin{aligned} P^{\rm PS}(\alpha) =& {\rm tr}(\hat{\rho}_{\rm out}\hat{M}) \\ =& \int \frac{d^2\xi_1}{\pi} \int \frac{d^2\xi_2}{\pi} \chi_{\rm A}^{\rm out}(\xi_1,\xi_2,0,0)(\pi\delta^2(\xi_1)-1). \end{aligned} \tag{16}$$

By substituting (8) into the above expression, we obtain

$$\begin{aligned} P_{\rm succ}(\alpha) =& 2P^{\rm PS}(\alpha) \\ =& \frac{4\big(g^2(2F_1+1)^2+2F_1(2F_1+1)+T|\alpha|^2\big)}{(g^2+1)(2F_1+1)^3} \\ & \times e^{-T\frac{|\alpha|^2}{2F_1+1}} - \frac{g^2}{(g^2+1)F_1} e^{-T\frac{|\alpha|^2}{2F_1}}, \end{aligned} \tag{17}$$

where $P_{\rm succ}(\alpha)$ is the total probability of success for the QS module, i.e., when either of D1 or D2 detector clicks. As expected, $P_{\rm succ}(\alpha)$ approaches, to first-order approximation, to $P_{\rm succ}^{\rm RL}(\alpha) = \mu + (1-\mu)|\alpha|^2 = (1+|g\alpha|^2)/(1+g^2)$, when $|\alpha| \ll 1$, at $\varepsilon = 0$ and $T = 1$.

This approximation is, however, invalid even when we slightly deviate from the condition on $|\alpha|$, as can be seen in Fig. 5(a). Here, we have plotted the exact probability of success, $P_{\rm succ}(\alpha)$, versus $|\alpha|^2$ and g, and compared it with the asymptotic value obtained by Ralph and Lund, $P_{\rm succ}^{\rm RL}(\alpha)$. It can be seen that the exact probability of success is always lower than the asymptotic value, and the difference is visible at all values of g. The success probability also increases with the decrease in g. For $|\alpha| \ll 1$, the success probability approaches its maximum possible value of $1/g^2$ [18]. But, again, as can be seen in Fig. 5(b), we quickly deviate from this ideal regime when $|\alpha|$ increases. This indicates that we cannot operate at maximum possible success probability for all possible inputs, as assumed in [16], if we use a QS as an NLA.

In Fig. 5(b), the maximum possible success probability, $1/g^2$, divides the plot into two regions. There is a region in which the success probability is above the maximum possible for an NLA. This implies that the QS operation should be very noisy in this region, hence breaking the assumption on the noise-free operation of the NLA. If we want to work in the region that $P_{\rm succ}(\alpha) < 1/g^2$, we will then have to deal with limitations on the maximum gain that we can choose for the range of input states we may expect. This indicates a trade-off between the amount of noise that the QS may add to the signal versus its gain and success probability. We will later address this issue, in the context of CV QKD, in our numerical results when we optimize the secret key generation rate over the system parameters.

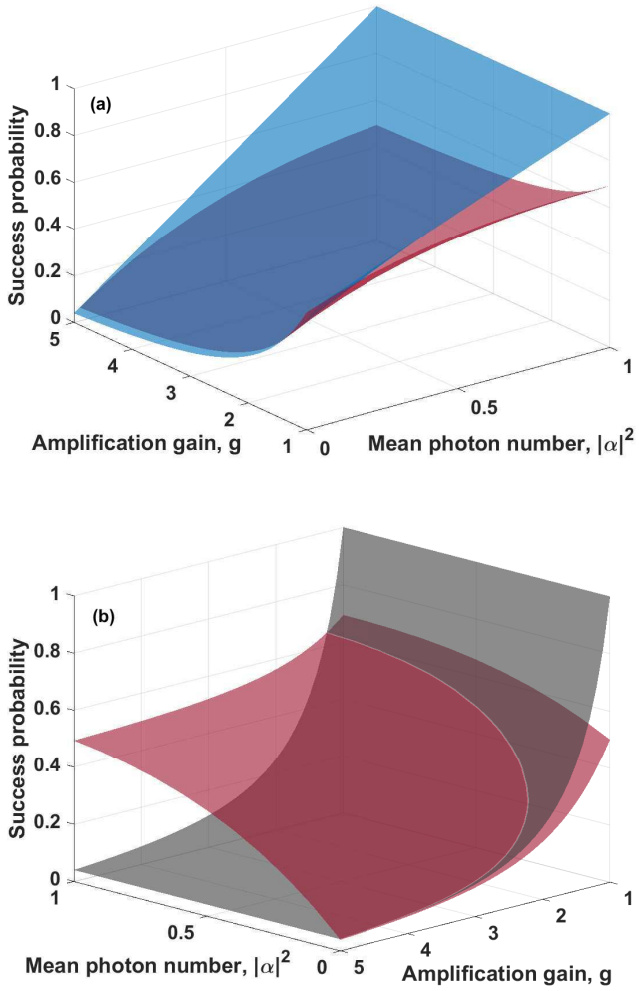

FIG. 5. (a) The exact success probability of a single QS (lower red), $P_{\rm succ}$, and that based on approximations in [20] (upper blue), $P_{\rm succ}^{\rm RL}$. (b) The exact success probability of a single QS (red), $P_{\rm succ}$, and that of an ideal NLA (grey), upper bounded by $1/g^2$, versus average photon number and amplification gain. In all cases, $\varepsilon = 0$ and $T = 1$.

D. Non-Gaussian behavior of the QS

Before calculating the secret key generation rate of a QS-equipped CV QKD system, it is necessary to better understand the nature of a quantum channel that includes a QS module. This is important because the majority of results on the secret key rate of CV QKD systems rely on Gaussian characteristics of the channel [35, 41]. This is not, however, the case for a QS module as we see in this section.

In order to examine the non-Gaussian behavior of the QS

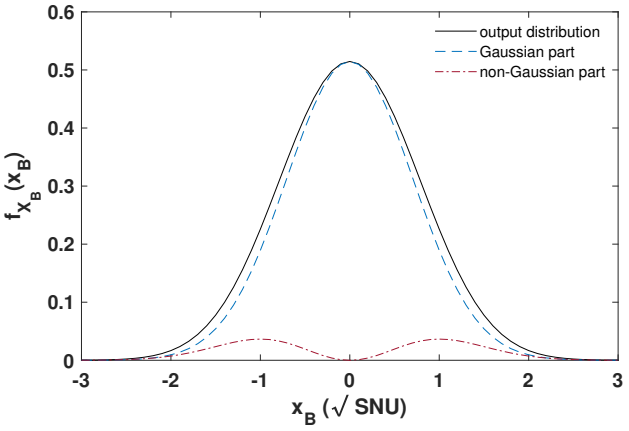

FIG. 6. The output distribution at the receiver side (solid-black), which comprises Gaussian (dashed blue) and non-Gaussian (dot-dashed red) parts. Here, $g = 2$, $V_A = 0.05$, $\varepsilon = 0$, and $T = 1$.

output, let us focus on the distribution of homodyne measurement results on quadrature $\hat{x}_B$. Let us also consider an input coherent state $|\alpha\rangle$, with $\alpha = x_A + ip_A$ as distributed by (1), at the QS port $\hat{a}_1$. That results in a thermal state with variance V_A and given by $\int d^2\alpha \frac{e^{-\frac{|\alpha|^2}{V_A/2}}}{\pi V_A/2} |\alpha\rangle_{\hat{a}_1}\langle\alpha|$. After performing similar calculations, the post-selected state will be given by

$$\hat{\sigma}_{\rm out}^{\rm PS}(V_A) = \sigma_{00}(V_A)|0\rangle_{\hat{b}_3}\langle 0| + \sigma_{11}(V_A)|1\rangle_{\hat{b}_3}\langle 1|, \qquad (18)$$

where

$$\begin{cases} \sigma_{00}(V_A) = \frac{8F_2}{(g^2+1)(2F_2+1)^2 P_{\rm succ}(V_A)} \\ \sigma_{11}(V_A) = \frac{4g^2}{(g^2+1)P_{\rm succ}(V_A)}\left(\frac{1}{2F_2+1} - \frac{1}{4F_2}\right) \end{cases} \qquad (19)$$

with success probability

$$P_{\rm succ}(V_A) = \frac{4}{(g^2+1)}\left(\frac{g^2(2F_2+1)+2F_2}{(2F_2+1)^2} - \frac{g^2}{4F_2}\right) \qquad (20)$$

and $F_2 = \frac{1}{2} + \frac{1}{4}T(V_A + \varepsilon_{\rm tm})$.

The probability distribution for obtaining a real number x_B after measuring $\hat{x}_B$, conditional on the success of the QS, is then given by

$$\begin{aligned} f_{X_B}(x_B) &= {\rm tr}(\hat{\sigma}_{\rm out}^{\rm PS}(V_A)|x_B\rangle\langle x_B|) \\ &= \left(\sigma_{00}(V_A) + 2\sigma_{11}(V_A)x_B^2\right)\frac{e^{-x_B^2}}{\sqrt{\pi}}, \end{aligned} \qquad (21)$$

where $\hat{x}_B|x_B\rangle = x_B|x_B\rangle$.

The expression for $f_{X_B}(x_B)$ will then have two components: one is a Gaussian term in x_B proportional to $\sigma_{00}(V_A)$, and the other is a non-Gaussian term proportional to $\sigma_{11}(V_A)$. Fig. 6 shows the contribution of each of these components in making $f_{X_B}(x_B)$ at $g = 2$, $V_A = 0.05$, $\varepsilon = 0$, and $T = 1$. We notice that even for such a small modulation variance, which corresponds mostly to small values of $|\alpha|$, the non-Gaussian term is quite distinct. Higher amplification gains could even result in more deviation from a Gaussian state. This non-Gaussian behavior would have ramifications on the key rate analysis of a QS-based system as we see next.

IV. SECRET KEY RATE ANALYSIS

In this section, we use the results in Sec. III to determine the secret key rate of the GG02 protocol when Bob uses a single QS before his homodyne measurement. We find the secret key rate in a nominal operation condition when no eavesdropper is present. We, however, assume a thermal loss channel with transmissivity T, modeled by a beam splitter, and an excess noise ε. This can effectively be thought as having an eavesdropper who attempts a Gaussian attack [42]. That is, we assume that Eve employs an entangling cloner by coupling one component of a TMSV state with Alice's signal, while retaining the other part for her future measurements. If one traces out the latter part of the TMSV state that Eve would keep for herself, the state on the other part would be a thermal state. The effective impact of Eves attack on the channel will then be equivalent to coupling Alices signal with a thermal state, which is the same as using a thermal-loss channel for analysing the secret key rate, as we have pursued in this work. It is important to note that such an attack may not be the optimal one for our non-Gaussian channel, but considering how close the output distribution in Fig. 6 is to a Gaussian distribution, the results obtained for this particular channel should not be far away from that obtained in an optimal attack [43]. The secret key rate of CV QKD protocols in the asymptotic limit of infinitely many signals is given by

$$K = \beta I_{\rm AB} - \chi_{\rm BE}, \qquad (22)$$

where β, $I_{\rm AB}$, $\chi_{\rm BE}$ are, respectively, the reconciliation efficiency, the mutual information between Alice and Bob, and eavesdropper's accessible information when reverse reconciliation is used.

In our proposed setup, since the QS operation is non-deterministic, the whole key rate formula should be multiplied by the *average* success probability of the QS, $\overline{P}_{\rm succ}$, where the averaging is performed over all possible inputs. Therefore, the secret key rate reads

$$K_{\rm QS} \geq \overline{P}_{\rm succ}(\beta I_{\rm AB}^{\star} - \chi_{\rm BE}^{\star}), \qquad (23)$$

where '$\star$' indicates that the mutual and Holevo information terms are calculated for the post-selected data when the QS is successful. The measurement results corresponding to unsuccessful QS events will be discarded at the sifting stage.

The fact that we only use the post-selected data for key extraction implies that we have to account for the non-Gaussianity of the QS output states. Unfortunately, the non-Gaussian behavior of the QS makes conventional methods for key rate calculation inapplicable. In order to take the non-Gaussian effects into account, we calculate the exact mutual information by directly using the conditional distribution of the QS output. Ideally one could also look for the exact calculation of the Holevo information term as well. But, this turns

out to be extremely cumbersome. Instead, in this paper, we find an upper bound for the Holevo information term by finding the covariance matrix (CM) of the output state from the total channel and then calculate the Holevo information for a Gaussian state with the same CM. The reason is that Gaussian collective attacks are proven to be optimal in the sense that they maximize the Holevo quantity [41] of fixed CM for the output shared state. Given the generality of the results in [41], in a real experiment, once we obtain the CM terms from the measurement results, we can use the same methodology to obtain a lower bound on the key rate.

In the following, we provide more detail on how each of the terms in (23) can be calculated.

A. Mutual information

The mutual information between two random variables X_A and X_B, corresponding to post-selected data on Alice's and Bob's sides, is the difference between the entropy function $H(X_B)$ and the conditional entropy $H(X_B|X_A)$ [44]:

$$I^{\star}_{\rm AB} = H(X_B) - H(X_B|X_A), \tag{24}$$

where

$$H(X_B) = -\int dx_B\, f_{X_B}(x_B)\log_2 f_{X_B}(x_B), \tag{25}$$

and

$$H(X_B|X_A) = -\int\int dx_A dx_B f(x_A,x_B)\log_2 f_{X_B}(x_B|x_A), \tag{26}$$

with $f(x_A,x_B) = f_{X_A}(x_A)f_{X_B}(x_B|x_A)$ being the joint probability density function.

Here, $f_{X_B}(x_B)$ can be obtained by using (21), while the conditional output distribution $f_{X_B}(x_B|x_A)$ can be obtained as follows:

$$f_{X_B}(x_B|x_A) = {\rm tr}(\hat{\omega}^{\rm PS}_{\rm out}(x_A)|x_B\rangle\langle x_B|), \tag{27}$$

where the conditional output state $\hat{\omega}^{\rm PS}_{\rm out}(x_A)$ is calculated in Appendix A. In our work, we numerically carry out the above integrals for a given set of parameters.

B. Holevo information

In order to calculate the Holevo information term, $\chi^{\star}_{\rm BE}$, we use the EB description of the protocol, where one part of an EPR state travels through the quantum channel and amplified by a QS, while the other is measured by Alice; see Fig. 7. In order to upper bound $\chi^{\star}_{\rm BE}$, what we need is then the CM of Alice-Bob bipartite state. We will then first derive the exact post-selected joint state, from which the CM parameters can be obtained. We use a similar approach to Sec. III in using characteristic functions to find a relationship between Alice and Bob states when the QS is successful. As shown in Fig. 7, we also account for the effect of the quantum channel loss and excess noise in our calculations.

By using (2) and the transformation matrix Γ, we can now write the full output antinormally-ordered characteristic function, including $\hat{a}_0$ mode, in terms of the input one by $\chi^{\rm out}_{\rm A}(\xi_0,\xi_1,\xi_2,\xi_3,\xi_{\rm N}) = \chi^{\rm in}_{\rm A}(\lambda_0,\lambda_1,\lambda_2,\lambda_3,\lambda_{\rm N})$, where

$$[\xi_0\ \xi_1\ \xi_2\ \xi_3\ \xi_{\rm N}] = \begin{pmatrix} 1 & 0 \\ 0 & \Gamma \end{pmatrix}[\lambda_0\ \lambda_1\ \lambda_2\ \lambda_3\ \lambda_{\rm N}],$$

with $\chi^{\rm in}_{\rm A}(\lambda_0,\lambda_1,\lambda_2,\lambda_3,\lambda_{\rm N}) = \chi^{\rm EPR}_{\rm A}(\lambda_0,\lambda_1)\times\chi^{\rm in}_{\rm A}(\lambda_2,\lambda_3,\lambda_{\rm N})$, where $\chi^{\rm EPR}_{\rm A}(\lambda_0,\lambda_1) = \exp\{-\delta^2(|\lambda_0|^2+|\lambda_1|^2) - 2{\rm Re}(\delta\gamma\lambda_0^*\lambda_1^*)\}$ is the antinormally-ordered characteristic function of the EPR state with parameters δ and $\gamma=\sqrt{\delta^2-1}$, and ${\rm Re}[\xi]$ being the real part of the complex number ξ. The term $\chi^{\rm in}_{\rm A}(\lambda_2,\lambda_3,\lambda_{\rm N})$ is calculated for input state $|1\rangle_{\hat{a}_2}\langle 1|\otimes|0\rangle_{\hat{a}_3}\langle 0|\otimes\int d^2\beta f_{\varepsilon}(\beta)|\beta\rangle_{\hat{a}_{\rm N}}\langle\beta|$.

Putting all this together, we then find the pre-measurement antinormally-ordered characteristic function for modes $\hat{a}_0$, $\hat{b}_1$, $\hat{b}_2$, $\hat{b}_3$, and $\hat{b}_{\rm N}$ as follows:

$$\begin{aligned}\chi^{\rm out}_{\rm A}(\xi_0,\xi_1,\xi_2,\xi_3,\xi_{\rm N}) =& e^{-\delta^2|\xi_0|^2}e^{-\kappa{\rm Re}\left(\xi_0^*(\xi_1^*-\xi_2^*)\right)} \\ &\times e^{-\frac{\delta^2 T}{2}|\xi_1-\xi_2-\sqrt{2}\tau\xi_{\rm N}|^2} \\ &\times e^{-\frac{1-T}{2}(1+\frac{\varepsilon}{2})|\xi_1-\xi_2+\frac{\sqrt{2}}{\tau}\xi_{\rm N}|^2} \\ &\times e^{-\frac{1-\mu}{2}|\xi_1+\xi_2-\frac{\sqrt{2}}{g}\xi_3|^2} \\ &\times e^{-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2} \\ &\times\left(1-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2\right),\end{aligned} \tag{28}$$

where $\kappa = 2\delta\gamma\sqrt{T/2}$.

In the EB scheme, we find the corresponding parameter δ in our EPR state, which gives the same output statistics for the signal that goes to Bob, when Alice does a heterodyne measurement on her state. It then turns out that to get an identical output state we should satisfy $\delta=\sqrt{(V+1)/2}$, where $V = V_A + 1$.

Having obtained the output characteristic function, we can find the corresponding output density matrix using (3). Then, by tracing out the output mode $\hat{b}_{\rm N}$ and also performing photon-detection measurements on modes $\hat{b}_1$ and $\hat{b}_2$—by introducing the same measurement operator as in (12)—we find the resultant joint state of $\hat{a}_0$ and $\hat{b}_3$ modes in the case of having a successful event.

Appendix B provides the detailed calculations of the post-measurement density matrix, and the corresponding CM parameters. It turns out that the CM of the shared bipartite state between Alice and Bob has the form

$$\gamma_{\rm AB} = \begin{pmatrix} a\mathbb{1} & c\sigma_{\rm z} \\ c\sigma_{\rm z} & b\mathbb{1}\end{pmatrix}, \tag{29}$$

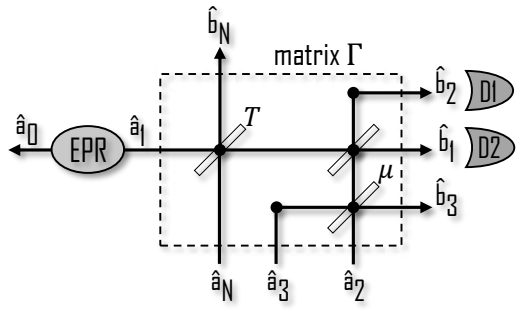

FIG. 7. QS-amplified EB CV QKD scheme. The quantum channel and the QS are considered as a combined system with input modes $\hat{a}_1-\hat{a}_3$ and $\hat{a}_{\rm N}$ and output modes $\hat{b}_1-\hat{b}_3$ and $\hat{b}_{\rm N}$. The transformation matrix of the system is given by (4).

where $\mathbb{1}=\mathrm{diag}(1,1)$ and $\sigma_{\rm z}=\mathrm{diag}(1,-1)$ with

$$\begin{aligned} a=&\Big(\frac{8[\gamma^2T+\big(2F_3+1-\gamma^2T\big)\big(g^2(2F_3+1)+2F_3\big)]}{(2F_3+1)^3}\\ &-\frac{g^2(2F_3-\gamma^2T)}{F_3^2}\Big)\frac{\delta^2}{(g^2+1)\overline{P}_{\rm succ}}-1,\\ b=&\frac{4}{(g^2+1)\overline{P}_{\rm succ}}\Big(\frac{4[g^2(2F_3+1)+F_3]}{(2F_3+1)^2}-\frac{g^2}{F}\Big)-1,\\ c=&\frac{8\delta\gamma}{(g^2+1)\overline{P}_{\rm succ}(2F_3+1)^2}g\sqrt{T}, \end{aligned} \tag{30}$$

$F_3=\frac{1}{2}+\frac{1}{4}T(2(\delta^2-1)+\varepsilon_{\rm tm})$ and $\overline{P}_{\rm succ}=\frac{1}{g^2+1}\big(4[(2F_3+1)g^2+2F_3]/(2F_3+1)^2-g^2/F_3\big)$.

It is interesting to make the following observation. If the EPR state is assumed totally uncorrelated, which happens when its squeezing parameter goes to zero, both parts of the state are left with vacuum states. Thus, if the QS is successful, the output state of mode $\hat{b}_3$ should be a vacuum state as well. This means that the CM of the end-to-end state is the identity [9]. We verify that in the case of having a totally uncorrelated EPR state, corresponding to $\delta=1$ and $\gamma=0$, the expressions above will indeed result in the identity matrix; that is, we obtain $a=b=1$ and $c=0$.

In addition, as a result of the statistical equivalence between EB and PM schemes, where $\delta=\sqrt{(V+1)/2}$, we conclude that $F_3=F_2$. Now that the CM is known, we can upper bound the Holevo information by using (B12).

V. NUMERICAL RESULTS

In this section, we present numerical simulations of the secret key rate of the QS-amplified GG02 protocol and compare it with that of the conventional one. We find the maximum value for the lower bound in (23) by optimizing, at each distance, the modulation variance, V_A, or, equivalently, the parameter δ in the EB scenario, as well as the QS parameter, μ, which specifies the QS amplification gain. We also account for the excess noise, as discussed in previous sections. We assume that the quantum channel between the sender and receiver is an optical fiber with loss factor α, whose transmittance is given by $T=10^{-\alpha L/10}$, where L is the channel length and the loss factor is $\alpha=0.2$ dB/km corresponding to standard optical fibers. Also, we assume $\beta=1$ and that ideal homodyne detection, with no electronic noise, is performed at the receiver.

We first highlight the importance of accounting for the non-Gaussian behavior of the QS by comparing the difference between the exact value of the mutual information function $I^{\star}_{\rm AB}$, given by (24), and that obtained by Gaussian approximation, $I^{\rm G}_{\rm AB}$, in (B13). Fig. 8 shows both curves, versus distance, at no excess noise. It is clear that the Gaussian approximation would have overestimated the mutual information between Alice and Bob at all distances considered, and that could have resulted in wrong bounds for the key rate of QS-based systems.

Figure 9 shows the optimized secret key rates of both conventional (solid lines) and the QS-assisted (dashed lines) GG02 protocol versus distance, as well as that of the PLOB bound for a repeaterless thermal-loss channel (labelled TL-PLOB) [45]. This is the bound given in (23) of [45] at an equivalent mean thermal photon number, $\bar{n}=\varepsilon_{\rm tm}T/(2(1-T))$, to our receiver excess noise (here at $\varepsilon_{\rm tm}=0.05$). There are several interesting observations that can be made in this figure. First, we note that for all considered cases, there exists a cross-over distance at which the QS-assisted curves surpass their corresponding no-QS curves. At $\varepsilon_{\rm tm}=0$, this happens at around 200 km. By increasing $\varepsilon_{\rm tm}$, the cross-over distance would drop and reaches around 150 km at $\varepsilon_{\rm tm}=0.05$. This proves the key objective of our work that, by using realistic NLAs, there would be certain regimes where NLA-based systems improve the performance and the distance at which secure keys can be exchanged.

It can be seen, in Fig. 9, that QS-equipped receivers may not support high key rates at short distances. In fact, except for the case of $\varepsilon_{\rm tm}=0$, we may not be able to exchange any secret keys at very short distances for the QS-based sys-

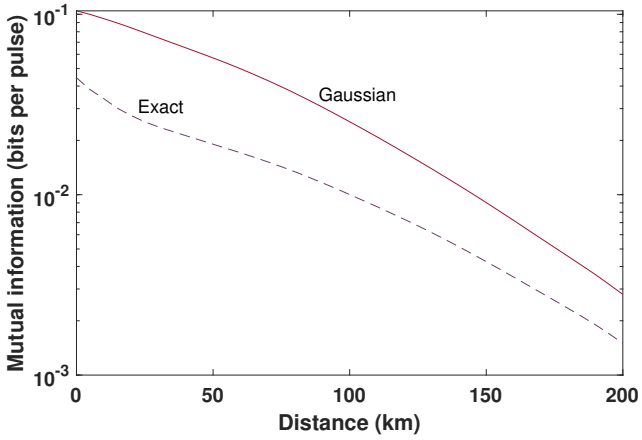

FIG. 8. The exact mutual information function (dashed) as compared to its Gaussian approximation (solid) versus distance at $\varepsilon=0$. All other parameters have been optimized.

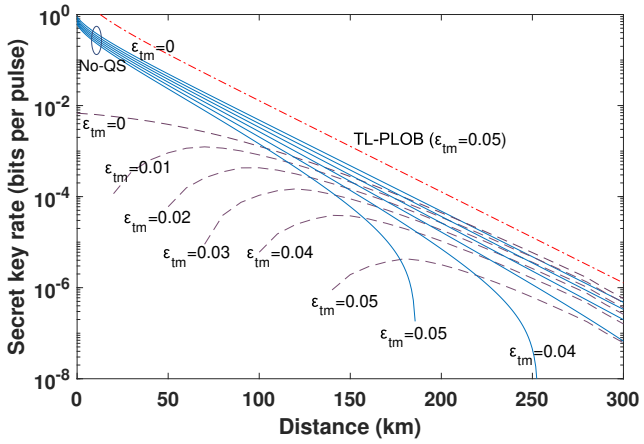

FIG. 9. The optimized secret key rate for the QS-amplified CV QKD protocol versus distance, as compared to the rate of conventional GG02, and the upper bound for a repeaterless thermal-loss channel (TL-PLOB) at a mean thermal photon number of $\varepsilon_{\rm rec}/(2(1-T))$. The solid lines represent the no-QS case with top curve at $\varepsilon_{\rm tm}=0$, and the bottom one at $\varepsilon_{\rm tm}=0.05$, and the middle curves covering $\varepsilon_{\rm tm}=0.01-0.04$

.

tem. Even for the no excess noise case, there are over two orders of magnitude difference between the no-QS and QS-based curves at $L=0$. This is attributed to multiple factors. First, the trade-off between the choice of modulation variance and noise level in the system, would require us to use very small values of V_A at short distances, otherwise the QS will not operate at its low-noise regime. For instance, at $L=0$, the optimum value of V_A for the QS-based system is 0.04. A no-QS system with such a low value of V_A also offers a low key rate of 2.83×10^{-2}, which is comparable to what we obtain for the QS-based system. Another factor is the success probability that at $L=0$ is around 0.5, and it almost linearly goes down to around 0.15 at 200 km. One last factor is also the fact that the QS is not entirely noise free. The additional noise by the QS would further decrese the rate at $L=0$. In addition to this, if we have nonzero values of excess noise, a combination of the above effects plus the external noise drive the key rate to zero at very short distances. This is by itself is not a practical dilemma, as, for a given channel length, one, in advance, can figure out whether to use a QS or not. But, this can affect the applicability of QS modules in a CV quantum repeater system.

Another observation in Fig. 9 is that, at long distances, the key rate for QS-based systems follows a parallel trend to that of the TL-PLOB curve. For instance, at $\varepsilon_{\rm tm}=0.05$, the key rate remains roughly one order of magnitude below the PLOB bound for long distances. We have numerically verified that, by optimizing system parameters, even for longer distances than shown on the graph, we can obtain positive key rates, albeit very low, for QS-assisted systems. The post-selection mechanism in the QS seems to be the key to obtaining positive key rates at long distances. At such distances, the channel loss naturally prepares low-intensity inputs to the QS, which

TABLE I. Optimized values for modulation variance and amplification gain at zero excess noise for the QS-based system.

Distance (km)	Optimized V_A	Optimized gain, g
0	0.05	1.00
100	0.8	1.36
200	3.5	2.38
300	11.5	4.36
400	12.5	14.1
500	13.5	100

allows us to use larger values of V_A, as shown in Table I. That would also enable us to use higher gains without necessarily increasing the QS noise. A higher-than unity gain for the post-selected states would then offer a better signal-to-noise ratio at long distances, which allows us to achieve positive secret key rates at longer distances than can otherwise be achieved for a no-QS system.

Figure 9 also shows that our QS-amplified system cannot beat the existing upper bound for repeaterless systems [45]. This agrees with the fact that any postprocessing at the receiver side does not change the repeaterless nature of the link, even though a form of amplification is in use. But, it will be interesting to see if, based on the above results, we can assess the practicality of the proposed CV repeater setups as in [27]. On the positive side, we can see that there exists a regime of operation where the slope of the QS-based curves offer a square root advantage as needed in repeater systems. On the downside, however, this behaviour only appears in a limited range of distance, and only up to a maximum value of excess noise. In our simulations, we were not able to obtain any positive secret key rates at $\varepsilon_{\rm tm}=0.06$, or higher. It seems that once the starting distance at which QS-based curves offer positive key rates lie above the maximum security distance for no-QS systems, it is no longer possible to get a positive key rate for QS-assisted systems. This may suggest that similar limitations might affect the suitability of CV repeater systems for QKD applications, which needs further investigation.

VI. CONCLUSION

In this work, we studied the performance of the GG02 protocol where the received signal was amplified by a quantum scissor. We first obtained the exact output state and success probability of the QS under study, which was later used in calculating the secret key generation rate of the system. We showed that the QS would turn a Gaussian input state into a non-Gaussian one. That would make the conventional techniques to estimating the key rate not directly applicable to our case. We instead directly calculated the mutual information by working out the probability distribution function of the quadratures after the QS. Also, in order to calculate the leaked information to Eve, we obtained the exact covariance matrix of the bipartite state shared between sender and receiver labs in the particular case of a Gaussian attack. We then found the Holevo information corresponding to a Gaussian shared output state with the same covariance matrix, which gives an

upper bound for the Holevo term in the case considered. We optimized the key rate over input modulation variance and amplification gain. Our results showed that, for a certain range of excess noise, the QS-enhanced system could reach longer distances than the no-QS system.

There are certain practical aspects that one should consider before using quantum scissors in CV QKD. One assumption that we make throughout our paper is that on-demand single-photon sources are available for our scheme. There are two practical issues, in this regard, that affect the performance of the QS-based system. The first is the rate at which single-photons are generated. The success rate of such sources directly affect the key rate achievable. Secondly, we should be cautious about the purity of the single-photon source output. Multiple-photon components, in particular, could be damaging to the performance of the QS. The good news is that the current available technology for quantum-dot sources has made a substantial progress to meet both above requirements. In particular, quantum dot sources with efficiencies over 80% and second-order coherence values < 0.004 have already been demonstrated [46, 47]. The second issue is the reliance on single-photon detectors, which will make CV QKD systems, in terms of requirements, similar to their discrete-variable counterparts. But, paying such prices may be unavoidable if one wants to have long-distance CV QKD and/or CV repeaters. Our study would, in particular, be highly relevant to analyzing the performance of recently proposed CV quantum repeaters [27], which rely on a similar building block. Moreover, one should note that all these additional equipment are at the receiver end of the CV-QKD link, which is often located at a network node, shared among many users. This can bring the total cost per user down to a reasonable value when the system is in widespread use.

We conclude by pointing out two additional remarks. First, note that, while the original NLA proposal by Ralph and Lund relies on multiple QS modules, in our scheme, we find using one QS is optimal as it minimizes the noise while we can adjust the signal level by optimizing the modulation variance. This also agrees with the results reported in [29], where they have shown that the reverse coherent information [48, 49] is maximum when one QS is used. Secondly, one may wonder about the similarities versus differences of an alternative approach to improving the rate-versus-distance behavior in CV QKD based on fighting noise by adding trusted noise [48, 50, 51] with the NLA solution. While, in our QS-based system, there are some elements of controlled noise by injecting the vacuum state into the QS module we believe that the key advantage of using a QS is in its underlying *post-selected* output. It will remain as an open question for future research to determine which of the two solutions are more effective in different scenarios, and if their impact can be combined to come up with more loss-resilient CV QKD implementations.

ACKNOWLEDGMENTS

The authors acknowledge partial support from the White Rose Research Studentship and the UK EPSRC Grant No. EP/M013472/1. S.P. would like to acknowledge funding from the European Unions Horizon 2020 research and innovation program under grant agreement No. 820466 (Continuous Variable Quantum Communications, 'CiViQ'). All data generated in this paper can be reproduced by the provided methodology and equations.

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, arXiv:1906.01645 (2019).

[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India, 1984) pp. 175–179.

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[6] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[7] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[8] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[9] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[10] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378.

[11] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).

[12] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).

[13] H. Yonezawa, S. L. Braunstein, and A. Furusawa, Phys. Rev. Lett. **99**, 110503 (2007).

[14] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J. ichi Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, Nat. Photon. **7**, 982 (2013).

[15] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[16] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).

[17] Y.-C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, and H. Guo, J. Phys. B: At. Mol. Opt. Phys. **47**, 035501.

[18] S. Pandey, Z. Jiang, J. Combes, and C. M. Caves, Phys. Rev. A **88**, 033852 (2013).

[19] D. T. Pegg, L. S. Phillips, and S. M. Barnett, Phys. Rev. Lett. **81**, 1604 (1998).

[20] T. C. Ralph and A. P. Lund, AIP Conference Proceedings **1110**, 155 (2009).

[21] E. Eleftheriadou, S. M. Barnett, and J. Jeffers, Phys. Rev. Lett.

111, 213601 (2013).
[22] J. Fiurášek, Phys. Rev. A **80**, 053822 (2009).
[23] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Photon. **4**, 316 (2010).
[24] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **104**, 123603 (2010).
[25] R. J. Donaldson, R. J. Collins, E. Eleftheriadou, S. M. Barnett, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **114**, 120505 (2015).
[26] M. Barbieri, F. Ferreyrol, R. Blandino, R. Tualle-Brouri, and P. Grangier, Laser Phys. Lett. **8**, 411.
[27] J. Dias and T. C. Ralph, Phys. Rev. A **95**, 022312 (2017).
[28] F. Furrer and W. J. Munro, Phys. Rev. A **98**, 032335 (2018).
[29] K. P. Seshadreesan, H. Krovi, and S. Guha, arXiv:1811.12393.
[30] J. Fiurášek and N. J. Cerf, Phys. Rev. A **86**, 060302 (2012).
[31] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, Phys. Rev. A **87**, 020303 (2013).
[32] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, Nat. Photon. **8**, 333 (2014).
[33] J. Zhao, J. Y. Haw, T. Symul, P. K. Lam, and S. M. Assad, Phys. Rev. A **96**, 012319 (2017).
[34] J. Bernu, S. Armstrong, T. Symul, T. C. Ralph, and P. K. Lam, Journal of Physics B: Atomic, Molecular and Optical Physics **47**, 215503.
[35] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).
[36] R. Kumar, H. Qin, and R. Allaume, New J. of Phys. **17**, 043027 (2015).
[37] N. A. McMahon, A. P. Lund, and T. C. Ralph, Phys. Rev. A **89**, 023846 (2014).
[38] J. Jeffers, Phys. Rev. A **82**, 063828 (2010).
[39] M. Navascués and A. Acín, Phys. Rev. Lett. **94**, 020505 (2005).
[40] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[41] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[42] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).
[43] M. He, R. Malaney, and J. Green, in *2018 IEEE Globecom Workshops (GC Wkshps)* (2018) pp. 1–6.
[44] T. M. Cover and J. A. Thomas, *Elements of Information Theory-Second Edition* (John Wiley and Sons, New Jersey, 2006).
[45] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[46] M. Müller, S. Bounouar, K. D. Jöns, M. Glässl, and P. Michler, Nat. Photon. **8**, 224 (2014).
[47] P. Senellart, G. Solomon, and A. White, Nat. Nanotech. **12**, 1026 (2017).
[48] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).
[49] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, Phys. Rev. Lett. **102**, 210501 (2009).
[50] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).
[51] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nature Communications **3**, 1083 (2012).

Appendix A: Conditional output state $\hat{\omega}_{\rm out}^{\rm PS}(x_A)$

In order to find the conditional output state when Alice has used an X quadrature value of x_A, we start with the input state in (6), and take an average over P_A with the input Gaussian distribution of $f_{P_A}(p_A) = e^{-\frac{p_A^2}{V_A/2}}/\sqrt{\pi V_A/2}$. As a result, the output characteristic function in (8) will also be averaged out and result in the following output state:

$$\begin{aligned}\hat{\omega}_{\rm out}^{\rm PS}(x_A) =&\omega_{00}(x_A)|0\rangle_{\hat{b}_3}\langle 0| + \omega_{01}(x_A)|0\rangle_{\hat{b}_3}\langle 1| \\ &+ \omega_{10}(x_A)|1\rangle_{\hat{b}_3}\langle 0| + \omega_{11}(x_A)|1\rangle_{\hat{b}_3}\langle 1|, \quad \text{(A1)}\end{aligned}$$

where

$$\begin{cases}\omega_{00}(x_A) = \frac{\widetilde{\omega}_{00}(x_A)}{P^{\rm PS}(x_A)} \\ \omega_{01}(x_A) = \omega_{10}^*(x_A) = \frac{\widetilde{\omega}_{01}(x_A)}{P^{\rm PS}(x_A)} \\ \omega_{11}(x_A) = \frac{\widetilde{\omega}_{11}(x_A)}{P^{\rm PS}(x_A)},\end{cases} \quad \text{(A2)}$$

with

$$\begin{cases}\widetilde{\omega}_{00}(x_A) = \frac{8F_1(2F_1+1)^2+TV_A(8F_1^2+6F_1+1)+2T(TV_A+4F_1+2)x_A^2}{(g^2+1)(2F_1+1)^{5/2}(TV_A+4F_1+2)^{3/2}} \\ \qquad\qquad \times \sqrt{2}e^{-\frac{Tx_A^2}{2F_1+1}} \\ \widetilde{\omega}_{01}(x_A) = -\frac{2g\sqrt{2T}x_A}{(g^2+1)(2F_1+1)^{3/2}\sqrt{TV_A+4F_1+2}}e^{-\frac{Tx_A^2}{2F_1+1}} \\ \widetilde{\omega}_{11}(x_A) = \frac{g^2}{g^2+1}\Big(\frac{2\sqrt{2}e^{-\frac{Tx_A^2}{2F_1+1}}}{\sqrt{(2F_1+1)(TV_A+4F_1+2)}} - \frac{e^{-\frac{Tx_A^2}{2F_1}}}{\sqrt{F_1(TV_A+4F_1)}}\Big) \\ P^{\rm PS}(x_A) = \widetilde{\omega}_{00}(x_A) + \widetilde{\omega}_{11}(x_A).\end{cases}$$

Appendix B: Covariance matrix elements

Having obtained the output antinormally-ordered characteristic function of (28), we use (3) to find the corresponding output state:

$$\begin{aligned}\hat{\rho}_{0123{\rm N}}^{\rm out} = \int \frac{d^2\xi_0}{\pi}\frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\frac{d^2\xi_3}{\pi}\frac{d^2\xi_{\rm N}}{\pi}\chi_{\rm A}^{\rm out}(\xi_0,\xi_1,\xi_2,\xi_3,\xi_{\rm N}) \\ \hat{D}_{\rm N}(\hat{a}_0,\xi_0)\hat{D}_{\rm N}(\hat{b}_1,\xi_1)\hat{D}_{\rm N}(\hat{b}_2,\xi_2)\hat{D}_{\rm N}(\hat{b}_3,\xi_3)\hat{D}_{\rm N}(\hat{b}_{\rm N},\xi_{\rm N}).\end{aligned}$$

In the following, we show how the shared state between Alice and Bob is found step-by-step. We first trace out mode $\hat{b}_{\rm N}$, see Fig. 7, to obtain

$$\begin{aligned}\hat{\rho}_{0123}^{\rm out} = \int \frac{d^2\xi_0}{\pi}\frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\frac{d^2\xi_3}{\pi}\chi_{\rm A}^{\rm out}(\xi_0,\xi_1,\xi_2,\xi_3,0) \\ \hat{D}_{\rm N}(\hat{a}_0,\xi_0)\hat{D}_{\rm N}(\hat{b}_1,\xi_1)\hat{D}_{\rm N}(\hat{b}_2,\xi_2)\hat{D}_{\rm N}(\hat{b}_3,\xi_3), \quad \text{(B1)}\end{aligned}$$

where we used ${\rm tr}[\hat{D}_{\rm N}(a,\xi)] = \pi\delta^2(\xi)$. Next, by defining the measurement operator $\hat{M} = (\mathbb{1} - |0\rangle_{b_1}\langle 0|)\otimes|0\rangle_{b_2}\langle 0|$, modes $\hat{b}_1$ and $\hat{b}_2$ are measured. The post-selected state is

$$\hat{\rho}_{03}^{\rm PS} = \frac{{\rm tr}_{12}(\hat{\rho}_{0123}^{\rm out}\hat{M})}{{\rm tr}(\hat{\rho}_{0123}^{\rm out}\hat{M})} =: \frac{\hat{\sigma}_{03}^{\rm PS}}{P_{\rm EB}^{\rm PS}}, \quad \text{(B2)}$$

where

$$\hat{\sigma}_{03}^{\rm PS}=\int\frac{d^2\xi_0}{\pi}\frac{d^2\xi_3}{\pi}\widetilde{\chi}_{\rm A}(\xi_0,\xi_3)\hat{D}_{\rm N}(\hat{a}_0,\xi_0)\hat{D}_{\rm N}(\hat{b}_3,\xi_3) \quad \text{(B3)}$$

with

$$\widetilde{\chi}_{\rm A}(\xi_0,\xi_3)=\int\frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\chi_{\rm A}^{\rm out}(\xi_0,\xi_1,\xi_2,\xi_3,0)\big(\pi\delta^2(\xi_1)-1\big), \quad \text{(B4)}$$

and $P_{\rm EB}^{\rm PS}=\overline{P}_{\rm succ}/2$ is the corresponding success probability to measurement $\hat{M}$:

$$\begin{aligned}P_{\rm EB}^{\rm PS}=&\int\frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\chi_{\rm A}^{\rm out}(0,\xi_1,\xi_2,0,0)\big(\pi\delta^2(\xi_1)-1\big)\\ =&\widetilde{\chi}_{\rm A}(0,0). \end{aligned}\quad \text{(B5)}$$

Now, we find the CM for $\hat{\rho}_{03}^{\rm PS}$. In doing so, we need to work out the triplet (a,b,c) of the corresponding CM as follows. By definition, assuming that $\hat{x}_0$ is the X quadrature of mode $\hat{a}_0$, we have

$$a=\langle\hat{x}_0^2\rangle_{\hat{\rho}_{03}}=\frac{\langle\hat{x}_0^2\rangle_{\hat{\sigma}_{03}}}{P_{\rm EB}^{\rm PS}}=\frac{{\rm tr}(\hat{\sigma}_{03}\hat{x}_0^2)}{P_{\rm EB}^{\rm PS}}, \quad \text{(B6)}$$

where

$$\begin{aligned}{\rm tr}(\hat{\sigma}_{03}\hat{x}_0^2)=&\int\frac{d^2\xi_0}{\pi}\frac{d^2\xi_3}{\pi}\widetilde{\chi}_{\rm A}(\xi_0,\xi_3)\\ &\times{\rm tr}[\hat{x}_0^2\hat{D}_{\rm N}(\hat{a}_0,\xi_0)]\times{\rm tr}[\hat{D}_{\rm N}(\hat{b}_3,\xi_3)]\\ =&\int\frac{d^2\xi_0}{\pi}\widetilde{\chi}_{\rm A}(\xi_0,0)\times{\rm tr}(\hat{D}_{\rm N}(\hat{a}_0,\xi_0)\hat{x}_0^2). \end{aligned}\quad \text{(B7)}$$

Assuming that $\xi_0=x+iy$, one can show that ${\rm tr}(\hat{D}_{\rm N}(\hat{a}_0,\xi_0)\hat{x}_0^2)=\pi\delta^2(\xi_0)+2\pi y\delta(x)\frac{d}{dy}\delta(y)-\pi\delta(x)\frac{d^2}{dy^2}\delta(y)$; thus,

$${\rm tr}(\hat{\sigma}_{03}\hat{x}_0^2)=-\widetilde{\chi}_{\rm A}(0,0)-\frac{d^2}{dy^2}\widetilde{\chi}_{\rm A}(0,y,\xi_3=0)\Big|_{y=0}, \quad \text{(B8)}$$

where we use the identity $\int dz f(z)\frac{d}{dz}\delta(z)=-\int dz\frac{d}{dz}f(z)\delta(z)$. Therefore,

$$a=-1-\frac{\frac{d^2}{dy^2}\widetilde{\chi}_{\rm A}(0,y,\xi_3=0)\Big|_{y=0}}{\widetilde{\chi}_{\rm A}(0,0)}. \quad \text{(B9)}$$

In a similar way, assuming $\xi_0=x+iy$ and $\xi_3=u+iv$, we show that

$$b=\frac{{\rm tr}(\hat{\sigma}_{03}\hat{x}_3^2)}{\widetilde{\chi}_{\rm A}(0,0)}=-1-\frac{\frac{d^2}{dv^2}\widetilde{\chi}_{\rm A}(\xi_0=0,0,v)\Big|_{v=0}}{\widetilde{\chi}_{\rm A}(0,0)} \quad \text{(B10)}$$

and

$$c=\frac{{\rm tr}(\hat{\sigma}_{03}\hat{x}_0\hat{x}_3)}{\widetilde{\chi}_{\rm A}(0,0)}=\frac{\frac{d}{dv}\Big[\frac{d}{dy}\widetilde{\chi}_{\rm A}(0,y,0,v)\Big|_{y=0}\Big]\Big|_{v=0}}{\widetilde{\chi}_{\rm A}(0,0)}. \quad \text{(B11)}$$

Having the integrals in (B4) taken, we are able to calculate the triplet (a,b,c), thus the CM. Using MAPLE, we obtain the closed form expressions as summarized in (30).

Having the triplet (a,b,c), $\chi_{\rm BE}^{\star}$ is upper bounded by:

$$\chi_{\rm BE}^{\rm G}=g(\Lambda_1)+g(\Lambda_2)-g(\Lambda_3), \quad \text{(B12)}$$

where

$$g(x)=(\frac{x+1}{2})\log_2(\frac{x+1}{2})-(\frac{x-1}{2})\log_2(\frac{x-1}{2})$$

and $\Lambda_{1/2}=\sqrt{(A\pm\sqrt{A^2-4B^2})/2}}=(\sqrt{(a+b)^2-4c^2}}\pm(b-a))/2$, $\Lambda_3=\sqrt{aB/b}}=\sqrt{a(ab-c^2)/b}}$, with $A=a^2+b^2-2c^2$ and $B=ab-c^2$. Note that (B12) is valid when we neglect the electronic noise at the receiver as we have assumed in our numerical results. Also, mutual information can be calculated form the covariance matrix, if we wish to use the Gaussian approximation, by

$$I_{\rm AB}^{\rm G}=\frac{1}{2}\log_2\frac{ab}{ab-c^2}. \quad \text{(B13)}$$